ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard

And

Risk Assessment

IEC 61511 Phase 1

Slide 3 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Requirements – Clause 8

A hazard and risk analysis shall be carried out on the process and its associated equipment. It shall result in:

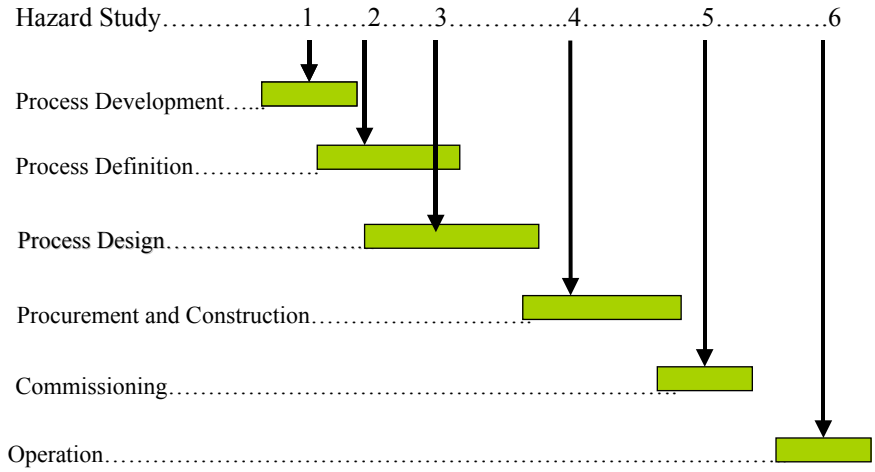
1. a description of each identified hazardous event and the factors that contribute to it (including human errors);
2. a description of the consequences and likelihood of the event;
3. Consideration of conditions such as normal operations, start up, shutdown, Maintenance, upsets, ESD
4. the determination of requirements for additional risk reduction necessary to achieve the required safety;
5. a description of the measures taken to reduce or remove hazards and risk;
6. a description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates and any credit taken for operational constraints or human intervention;
7. Allocation of the safety functions to layers of protection taking into account the impact of common cause failures between safety layers
8. identification of those safety functions applied as SIFs

Slide 3 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard Studies

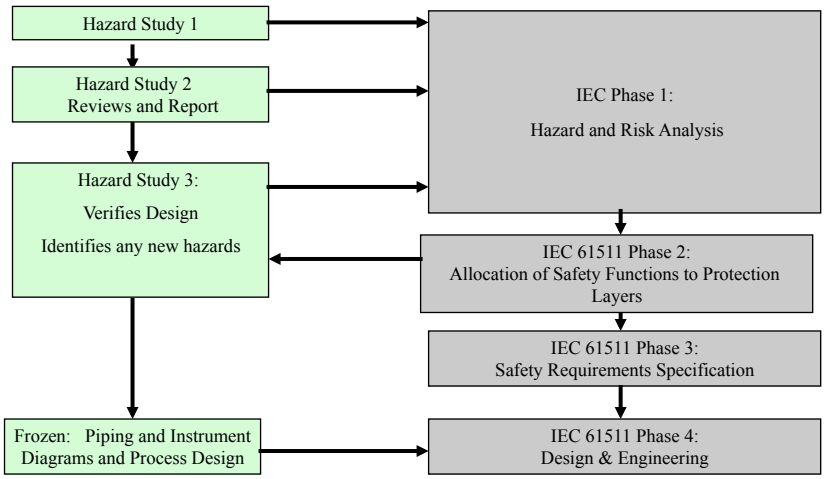


ProSalus Limited Slide 3 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Activity Model: Hazard Studies and Safety Lifecycle Phases



ProSalus Limited Slide 3 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard Study 1

- Identify hazards associated with the process.
- Identify major environmental problems and assess suitability of proposed sites
- Criteria for hazards, authorities to be consulted, standards and regulations, codes of practice.
- Collect/review information on previous hazardous incidents.

Also known as: Concept and definition phase hazard study or Screening Level Risk Analysis (SLRA)

ProSalus Limited Slide 3 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

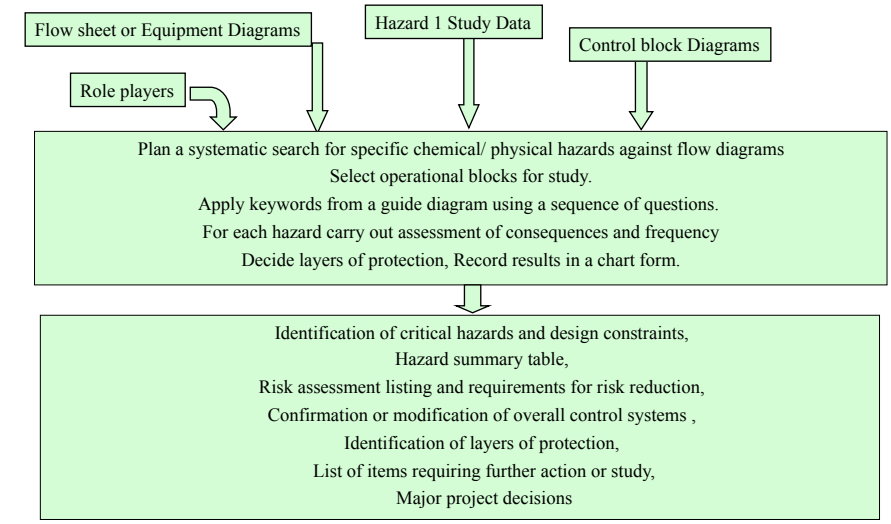
Process Hazard Study 2

- Examine plant items and equipment on process flow sheet and identify significant hazards
- Identify areas where redesign is appropriate
- Assess plant design against relevant hazard criteria
- Prepare environmental impact assessment

ProSalus Limited Slide 3 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Measures to prevent or eliminate causes

Measure	Reduce hazard due to
Pressure/temperature reduction in process	High energy levels, stresses
Minimize equipment, piping, seals and joints	Leaks
Design for containing maximum pressure	Rupture/bursting
Provide pressure relief system	Rupture/bursting
Location/layout/spacing	Interactions/confined spaces
Operational alarms	Wrong operating conditions
Automatic protection systems (SIS)	Wrong operating conditions, dependency on human response

ProSalus Limited

Slide 3 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Measures to mitigate or reduce consequences

Measure	Mitigate Consequences of
Containment/bunding/safe disposal	Uncontrolled dispersion, contamination
Rapid leak detection	Leaks leading to gas cloud /liquid pool
Rapid fire detection	Runaway Fire
Control room/occupied buildings design for pressure shocks	Injury to occupants
Toxic refuge (Gas safe room)	Toxic vapour exposure
Fire protection/dispersion aids – water jets	Spread of fire
Fire fighting facilities	Uncontrolled fire
Off site vent/ Relief discharges	Uncontrolled emissions
Isolation of stages and units	Migration of fires Feeding of fires from other units
Emergency procedures	Uncontrolled responses Chaotic evacuation
Emergency shutdown systems	Slow response to hazardous event. Dependency on human factors

ProSalus Limited

Slide 3 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Process Hazard study level 3

- Critical examination of plant operations on completed design
- Identifies detail hazard, control and operability problems.
- Reviews existing safety measures
- Often uses Hazard and Operability study (HAZOP) method
- Should be completed before detailed design/ procurement begins

ProSalus Limited

Slide 3 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Overall HAZOP Study procedure

Definition Phase
Scope & objectives-- Responsibilities--Select team

Preparation Phase
Plan--Collect Data--Choose recording method
Estimate time required- Arrange the schedule

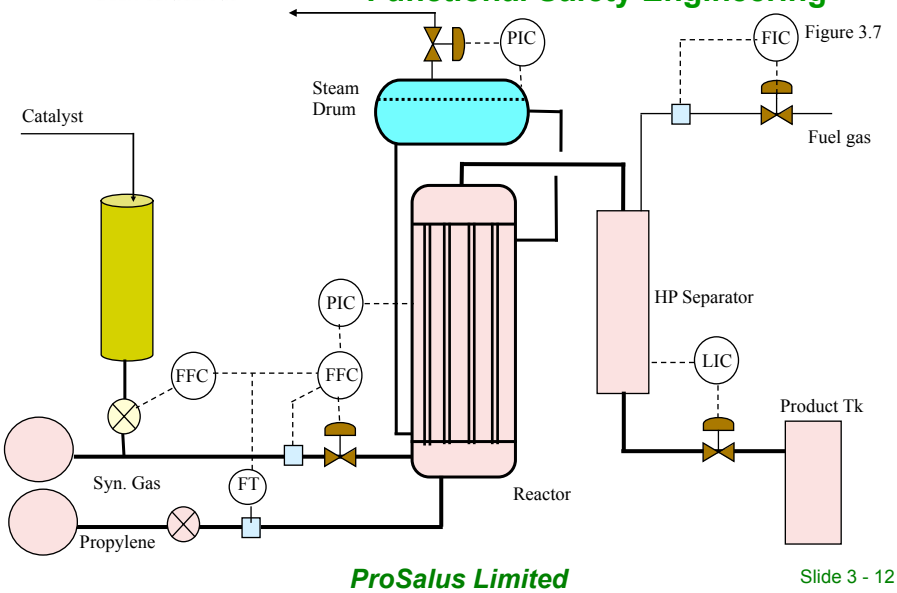
Examination Phase
Divide system into elements--Examine element for deviations from design intent
Identify possible deviations, cause, consequences, protection needs
Agree actions -repeat for each element

Reporting and Follow-up Phase
Record on worksheets--Sign off records--Produce report
Follow up actions - Restudy where needed- Issue final report

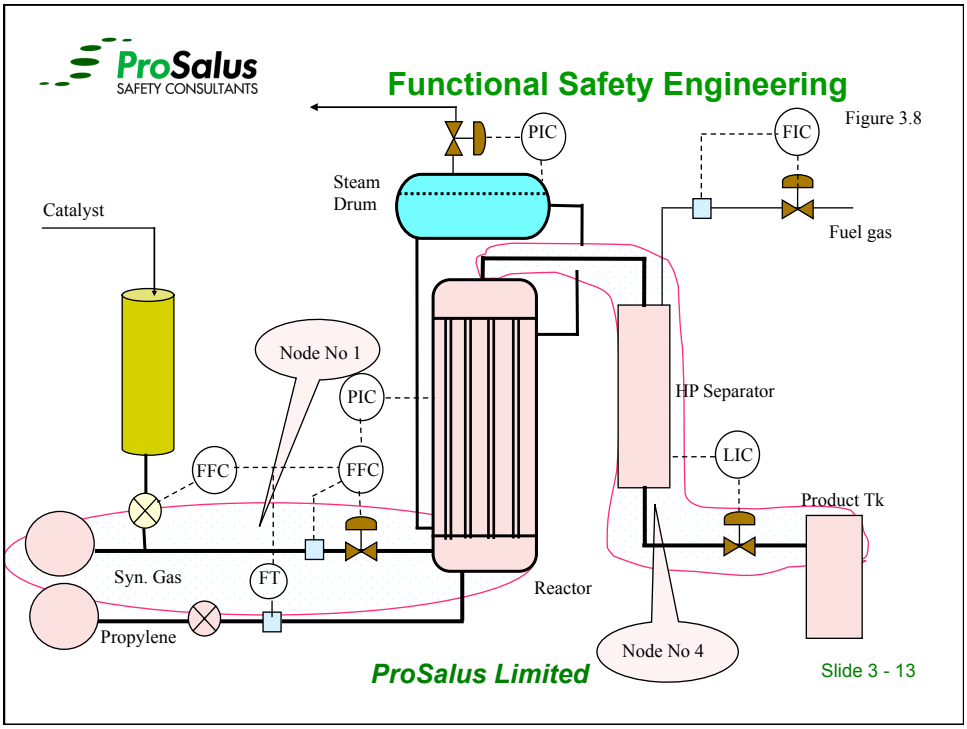
ProSalus Limited Slide 3 - 11

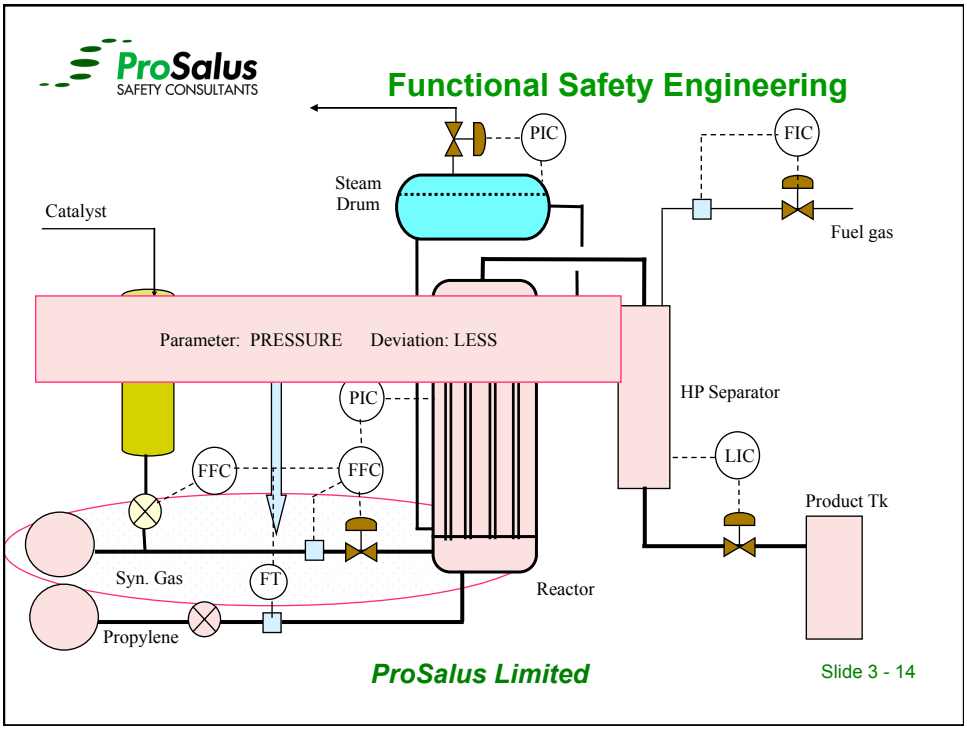
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited Slide 3 - 12





ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Line by Line Study

- Obtain a description of the intended normal modes of operation from the designer.
- Apply a series of prompts using keywords to stimulate thinking by the whole team about deviations from normality.
- Record those deviation conditions that are possible and are likely to have a significant consequence in terms of hazards or damage to the plant or severe loss of production.
- Record the corresponding actions required of the design team or the plant management as appropriate.

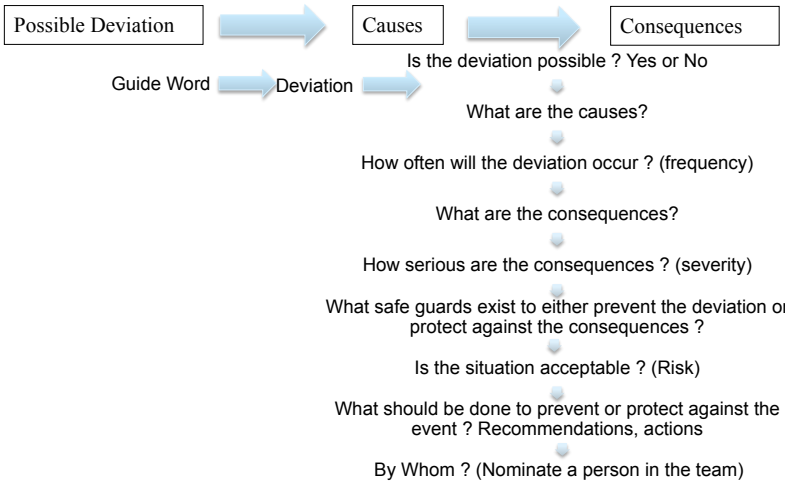
ProSalus Limited

Slide 3 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Causes and consequences



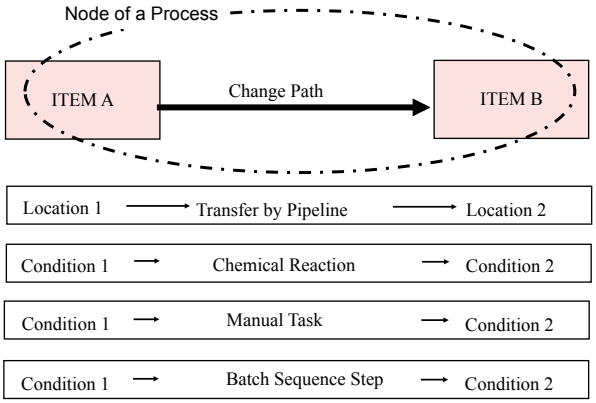
ProSalus Limited

Slide 3 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Change Path Concepts



ProSalus Limited

Slide 3 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Generating deviations

Basic Guidewords

Guideword	Meaning
NO or NOT (or none)	None of the design intent is achieved
MORE (more of, higher)	Quantitative increase
LESS	Quantitative decrease
AS WELL AS (more than)	Qualitative modification or additional activity occurs
PART OF	Only some of the design intent is achieved.
REVERSE	Logical opposite of design intent
OTHER THAN	Complete substitution – another activity takes place.

ProSalus Limited

Slide 3 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of Derived Guidewords for Process Studies

Parameter	Guidewords that can give a meaningful combination
Flow	Non; more of; less of; reverse; elsewhere, as well as
Temperature	Higher; lower
Pressure	Higher; lower; reverse.
Level	None; higher; lower
Mixing	Less; more; none.
Reaction	Higher (rate of); lower (rate of); none; reverse; as well as.
Phase	Other; reverse; as well as.
Composition	Part of; as well as.
Communication	None; part of; more of; less of; other; as well as.

ProSalus Limited

Slide 3 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Creating Deviations

Combining guidewords with elements generates deviations, some of which are credible and some are not credible.

Guideword + Element → Possible Deviation

The multi disciplined (Process, Operations, Maintenance etc) HAZOP study team has the task of deciding what elements are applicable and then deciding what deviations are credible for each element

ProSalus Limited

Slide 3 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of guideword/element matrix for process example

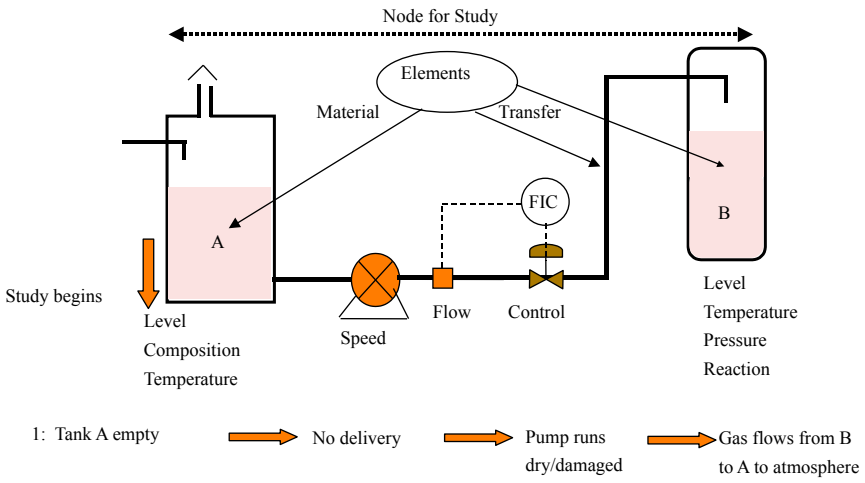
Element (parameter)	Guidewords								
	No	More	Less	Rev.	Part of	As well as	Where else	Early/ late	Other
Tank A Level	X	X	X						
Tank A Comp		X	X			X			
Flow in pipe	X	X	X	X		X			
Temp in pipe		X	X						
Pressure in pipe	X	X	X						X

ProSalus Limited

Slide 3 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Examples of Element First Examination Method

Part : Transfer of acid from A to B	Element: Tank A	Parameter: Level	
Deviation	NONE	**Meaning/effect:**	Tank is empty
Is it possible	YES		
Causes	1:No supply	2: Extraction exceeds inflow.	3:
How often?	Monthly	Monthly	
Consequences	1: No transfer	2: Pump damage	
Severity	Nil	Moderate+ Loss of production	
Safeguards	Operational	None	
Acceptable risk	N/A	NO	
What should be done		Low level detection and interlock on pump	
Action:	Specify safety trip	Process and Instrument engineers.	

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Causes of Deviations

The cause of a deviation will nearly always be due to a failure of some kind

- Hardware: Equipment, piping, instrumentation, design, construction, materials
- Software: Procedures, instructions, specifications
- Human: Management, operators, maintenance
- External: Services (steam, power), natural (rain, freezing), sabotage.

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Evaluating EUC Risks

- Safeguards will probably be in place …
- How do we describe the risks ?
  - Pretend there are no safeguards
  - Identify deviations and causes
  - Identify consequences, again without protection.
  - Recognize the protection measures provided (describe the safeguards)
  - Decide if the protection measures are good enough.

ProSalus Limited Slide 3 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 4 - Purpose

Reservation review verifying that the provisions in all previous studies are fully implemented and that the installation has been implemented as per the design intent

- **Key Aspects**
  - Hazard review after construction is substantially completed but before hazardous materials are introduced to the plant
  - Check that equipment and installation is as per design intent
  - Check that previous Hazop Study actions are closed out
  - Emergency Plan and Operating and maintenance instructions / procedures have been handed over and are in place
  - Safety manual handed over
  - Staff training and competency assessments are complete

ProSalus Limited Slide 3 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 5 - Purpose

Safety Health and Environmental audit of constructed plant before introducing hazardous materials to provide an opportunity for those responsible for personal safety, employee health and environmental protection on the site to satisfy themselves that the detailed implementation of the project meets the company, statutory and legislative requirements.

- **Key Aspects**
  - Hazard Review to ensure that safety, health and environmental management systems and procedures are in place
  - Process Safety Indicators have been identified and added to SMS
  - SIFs have been added to Site Risk Control Systems
  - Emergency Plan and Operating and maintenance instructions / procedures have been handed over and are in place are operational

ProSalus Limited Slide 3 - 27

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hazard Study 6 - Purpose

Ongoing review through out the plant life time to confirm that design has been fulfilled opposite SHE aspects and compare plant operational experience with assumptions made in hazard studies. First review will include confirmation that all documentation is available and in place.

- **Key Aspects**
  - First review 6 -12 months after plant operation
  - Validation that all documentation has been updated
  - Modifications made during commissioning and start up have not altered the risk profile
  - Validation of compliance to conditions of consent
  - Validation of employee occupational health monitoring

ProSalus Limited Slide 3 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

HAZOP Examples

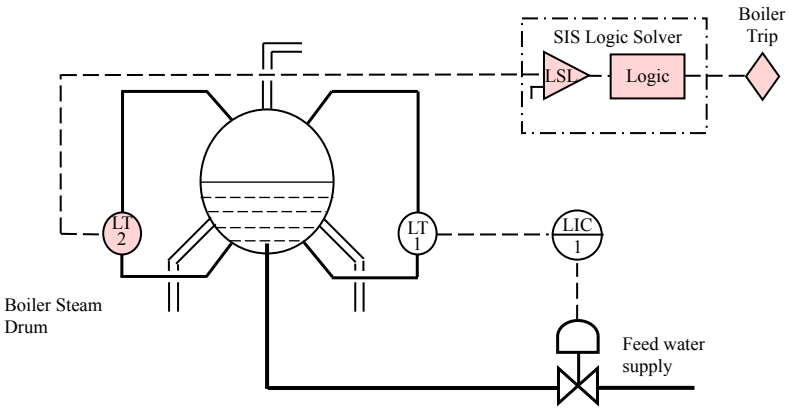
ProSalus Limited

Slide 3 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of a safeguard in place: Boiler drum level



ProSalus Limited

Slide 3 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Worksheet Example for Drum Level Hazard

Part : Boiler feedwater to drum	Element: Drum	Parameter: Level	
Deviation	LESS	Meaning/effect:	Drum level runs very low or empty
Is it possible	YES		
Causes	1:Loss of feedwater supply	2: Instrument fault, sensor reads high	3: Control valve fails shut
How often?	1 per yr	0.2 per yr	0.1/yr
Consequences	1: Boiler tubes overheat and rupture		
Severity	Severe. Risk of injuries	Severe: Damage to boiler	
Safeguards	Low feedwater pressure alarm	Low level trip system	
Acceptable risk	subject to satisfactory assessment		
What should be d one	Risk assessment to check safeguard performance		
Action:	Prepare safety requirements spec.	Determine target SIL rating of trip and alarm	

ProSalus Limited

Slide 3 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Complementary Hazard Study Techniques

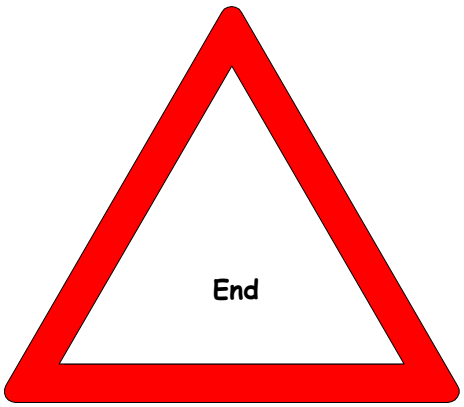
- Mechanical Plant, Instrumentation and Machines – FMEA, FMECA & FMEDA
- Electrical systems – E-HAZOP / Sneak Analysis
- Control systems - CHAZOP
- Alarm systems – Alarm Review – EEMUA 191
- Operation & Maintenance Tasks – Hierarchical Task Analysis
- Human HAZOP - Predictive Human Error Analysis (PHEA)

ProSalus Limited

Slide 3 - 32

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 3 - 33